IoT Based Smart Plugs and their Vulnerabilities

[1]Sameer P Raut, [2] S V. Athawale

[1]T.E. Student, [2]Assistant Professor
Department of Computer Engineering
[1]AISSMS College of Engineering, Kennedy Road, Pune-411001, India

***Abstract*—Balancing Energy production and day by day increasing demand is becoming challenging task. Energy Management Systems are used for more efficient use of Electrical energy. One such component of Energy Management Systems is Smart Plugs. The underlying technology behind Smart plugs is the Internet of Things (IoT).The easiest way to make any electronic device Smart is to join it through Smart Plugs. Smart Plugs can be used to get detailed information about current drawn, connection point voltages, remotely turning it on and o_ of plugged devices etc. Smart plugs have been deployed heavily in recent years as a need for Home Automation. However, they have capabilities to pose serious vulnerable problems if they are not investigated thoroughly. Such problems linked to Smart Plugs have been left open Knowingly or unknowingly.**

***Index Terms*—Internet of Things, Smart Plugs , Vulnerabilities, Counter Measures.**

---

1. INTRODUCTION

The Internet of Things (IoT) is multiplying at the rapid rate, and it is becoming more and more important for professionals to understand what it is, how it works, and how to capture its power to improve business. We will look at the things that make up the Internet of Things, including how those components are connected together, how they communicate, and how they generate data. We are going to examine security threats and privacy issues and highlight how IoT can optimize processes and improve efficiencies. IoT devices are a part of the larger concept of home automation, also known as domotics. Large smart home systems utilize a main hub or controller to provide users with a central control for all of their devices. These devices can include lighting, heating and air conditioning, media and security systems. Ease of usability is the most immediate benefit to connecting these functionalities. Long term benefits can include the ability to create a more environmentally friendly homeby automating some functions such as ensuring lights and electronics are turned off.

2. ARCHITECTURE

Smart Plug Registration Phase

When the plug connects to an outlet and powers up for the first time, it works as a wireless access point (AP). We call it the plug AP to differentiate it from a home wireless router. A user can use her smartphone to connect to the plug AP. After the smartphone is associated with the plug AP, the smartphone Searches the home wireless router and can connect the plug to the home wireless router. Once the plug can access the Internet, it will register with a remote authentication server. The detailed procedure is introduced as follows.

Plug and Controller in the Same WLAN :

Assume that the plug and controller are in the same wireless local area network. The detailed authentication process between the plug and the controller is introduced below.

STEP 1a : The controller sends a UDP request with a command type of 1030 to the authentication server. The UDP port of the authentication server for the controller is 8766. The request packet contains a credential in the auth value held for authentication and information of the MAC address. The credential consists of the user account and password. The format of this value is username: password.

STEP 2a : In this step, the authentication server processes the UDP request and forwards it to the right smart plug. Once receiving the datagram request from the controller, the authentication server first checks the status of the plug with the MAC address sent from the controller.

STEP 3a : In this step, the smart plug authenticates the controller and sends back a datagram response to the authentication server. After receiving the request from the authentication server, the smart plug will check the credential to authenticate the identity of the remote controller.

STEP 4a : In this step, the authentication server forwards this datagram response packet (except the 1120 packet) to the controller. Upon receiving the UDP response from the plug, the authentication server modifies the command type to 1070, adds additional information, and then forwards the response package to the controller. The additional information includes the IP address and port of both the plug and the command relay server, the relay ID, and the information of the plug including the model, type, alias, firmware version, etc.

STEP 5a : Both the smart plug and the controller establish TCP connections to a rendezvous server deployed in the cloud server. We call this server as a command relay server as it is used to relay the commands between plugs and controllers.

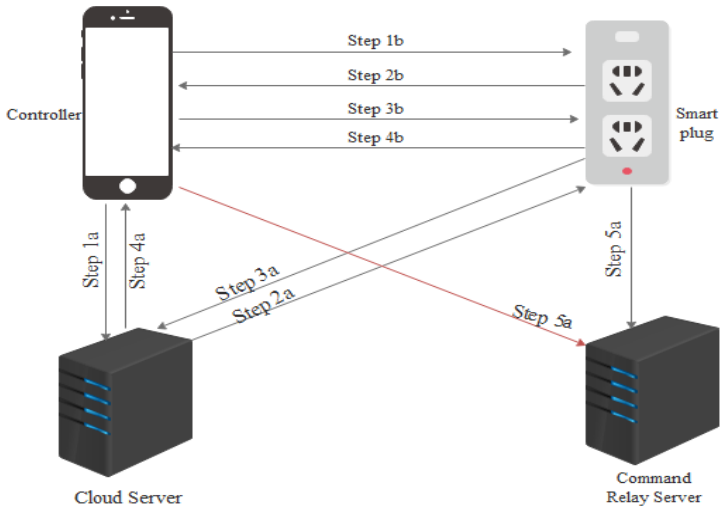
STEP 1b : Once a controller manages to connect to a WLAN, the controller broadcasts two consecutive 22-byte datagram packets in order to determine if the plug and the controller are in the same WLAN. These packets are used for discovering the plug, in case both the plug and controller are located in the same WLAN. The destination port of these broadcast packets is 20560. The

controller also continues the authentication phase introduced in Section III-B1 sending the credential to the smart plug via the remote authentication server.

STEP 2b : Upon receiving the broadcast datagram packets, the plug will respond immediately. The plug sends back a datagram packet to the controller. The information in the packet includes model, MAC address, IP address, and firmware version, and alias of this plug. In this way, both the plug and the controller know that they are located in the same WLAN.

STEP 3b : The controller establishes a TCP connection to a server deployed on the plug and leverages the HTTP protocol to communicate with the local smart plug. The destination port of this HTTP server is 10000. Once the TCP connection is built, the controller sends the authentication information, i.e., user name and password, using the HTTP basic authentication method. The payload contains a get command to obtain the state of the plug so that the app will be able to display the Current status of the plug.

STEP 4b : The smart plug responds with a HTTP packet to the controller. The message shows the state of the power, (i.e., on or o_). The controller obtains this response message and shows the information to the user via the app. Therefore, after the authentication phase, the user can perform various controls Operations through the app. For instance, the user can reset the password or the SMTP server.



3. VULNERABILITIES OF SMART PLUGS

a. Device Scanning Attack

In a device scanning attack, the attacker can scan all plugs by enumerating possible MAC addresses of the smart plugs from this vendor. According to recent research, many users do not change the default password after deploying their IoT devices. They expect the vendor takes care of the security. The key to a successful device scanning attack is to know the MAC address space of the smart plug. Luckily for the attacker (unluckily for the manufacturer), MAC addresses are predictable.

We can search the MAC address spaces allocated to a company/manufacturer on the Internet. The first 6 digits of a MAC address indicate the device manufacturer and the other 6 digits refer to a special MAC address given to the manufacturer. A manufacturer often gives a block of sequential MAC addresses to the same product. Therefore, if we buy a few smart plugs, we can guess at least portions of MAC addresses allocated to smart plugs of this model. The attacker can enumerate the whole MAC address space of a Manufacturer in a brute force attack.

b. Brute Force Attack

After deploying the scanning attack, the attacker can discover all the online plugs using non-default passwords. Then the attacker can select those plugs, construct 1030 packets, and enumerate all possible passwords. The attacker just needs to wait until she receives the right response. At the time of the writing, our experiments show that the authentication server does not block this brute force password attack. However, our experiments show that the plug system actually allows a password of 20 characters, including digits and upper-case and lower-case alphabetic letters. This password policy is not written in any of the provided manual and we cannot find it online either. If a user indeed inputs a long and complicated password, the brute force Attack does not work anymore. Unluckily, the plug system suffers from the following device spoofing attack, which can expose any plug credential.

c. Device Spoofing Attack

1) Attack Process: In the device spoofing attack, we create a software bot that mimics a plug and performs the authentication with the remote controller in order to directly obtain the credential from the controller. It works as follows.

a) The attacker first selects a target plug with a special MAC address. Recall the attacker knows this plug is online and this plug does not use the default password by using the device scanning attack. If the attacker has sufficient resources, she can simultaneously choose as many targets as she wants.

b) The attacker registers the spoofed plug by performing STEP 3 in. In particular, the attacker can emulate the communication behavior of a real plug and send a packet with a command type of 1010 to the authentication server. Since the server does not provide any authentication method to authenticate the plug, it registers this spoofed plug and sends back the response packet with the command type of 1020 as introduced in STEP 4. At this point, the spoofed plug is online.
c) When a victim opens her app on the smartphone, the app will automatically send the 1030 packet to the authentication server as introduced in STEP 5a.The authentication server will forward this message to the attackers spoofed plug as introduced in STEP 6a. Since the 1030 packet contains the credential, the attacker can effectively derive the credential.

2) Issues: In the spoofing attack, the real plug sends the 1010 packet to the authentication server every 20 minutes in order to keep its online status. To address this issue, the attacker should periodically send 1010 packets to the authentication server so as to keep the spoofed plug online. The attacker may want to keep the spoofed plug online as long as possible in order to increase the success rate of the attack.

d. Firmware Attack

The attacker can install a malicious firmware on the smart plug so that she can remotely control it. Once the malicious firmware is installed to the plug, it can establish a reverse tunnel back to a remote malicious server and open a reverse shell. Therefore, the attacker can remotely access the plug system and perform further attacks, e.g. installing various malware into the plug. In this attack, we assume the attacker can access the local network of the plug and monitor the traffic between plug and controller so as to derive the encoded Wi-Fi username and password in the HTTP header. The attacker can then leverage the username and password for the authentication purpose and upload the malicious firmware to the HTTP server on the plug. The attacker is capable of modifying the firmware in order to add the malicious functionality since the vendor of the smart plug provides the open source code of the firmware.

4. DEFENSE STRATEGIES

a. Secure Communication Protocol

Cryptography has to be employed to encrypt communication. Encoding and obfuscation are not enough to provide secret communication. We can see that an attacker can crack the obfuscation algorithm by analyzing the network traffic. With an eavesdropping attack, she can observe all the plaintext transmitted between the plugs and the controller. To mitigate these threats, secure communication protocols should be adopted, e.g., DTLS, TLS/SSL, and HTTPS, to encrypt the content transmitted between the plug, the controller, the authentication server, and the command relay server.

b. Intrusion Detection System

To thwart the scanning attack, an intrusion detection system should be employed at the server side. The intrusion detection system should be able to identify extensive scanning attacks. For example, it should detect the continuous and rapid password attempts. Moreover, the intrusion detection system can be used to detect abnormal behaviors. For instance, during the spoofing attack, the authentication server can identify the attack by simply tracking the geolocation of the registered plugs. If the geolocation information shows that two consecutive Physical locations of a registered plug are far away in a short time period, the spoofing attack may be underway.

C. Anti Bot Mechanism

To prevent the brute force attack, the authentication server should adopt methods to determine if the login is performed by a human or a bot. For instance, the CAPTCHA can be used to mitigate the brute force attack conducted with bots. Limiting the number of login attempts can be an effective way to prevent this type of attack.

5. LITERATURE SURVEY

[1] **Zhen Ling; Junzhou Luo; Yiling Xu; Chao Gao;KuiWu and Xinwen Fu,[1]** "*Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System"* The Authors have demonstrated security problems in Edimax Plugs and sent a compelling message Edimax plug and other IoT device manufacturers to enhance the security of their systems. Vulnerabilities of Edimax Plugs were put forth by reverse engineering its communication protocols.

[2] **O. Arias, J. Wurm, K. Hoang, and Y. Jin,[2]** "*Privacy and security in internet of things and wearable devices, IEEE Transactions on Multi-Scale Computing Systems*. The Authors had demonstrated a non-secure hardware platform will inevitably lead to a non-secure software stack. Furthermore, without being able to authenticate the running software, it cannot be trusted to make decisions about its own validity.

[3] **I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, and M. Gruteser,[3]***" Neighborhood watch: Security and privacy analysis of automatic meter reading systems"* The Author has proposed that currently deployed AMR systems are vulnerable to spoofing attacks and privacy breaches.

[4] **Q. Yang, J. Yang, D. A. W. Yu, N. Zhang, and W. Zhao,[4]**" *A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications"* The Authors have presented the traditional three-layer architecture and the SoA- based four-layer architecture. In addition, to secure IoT, potential security and privacy issues that could affect the effectiveness of IoT, and their potential Solutions has been presented.

[5] **S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini,[5]** "*Security, privacy and trust in internet of things: The road ahead*, Chichester" The Authors had proposed that Traditional security countermeasures cannot be directly applied to IoT technologies due to the different standards and communication stacks involved.

[6] **M. Rahman, B. Carbunar, and M. Banik,[6]** "*Fit and vulnerable: Attacks and defenses for a health monitoring device"*. The Author had took into consideration the Fitness Band Fit-Bit. In this case study he proposed that the integration of health data into social networks is fraught with privacy and security vulnerabilities.

CONCLUSION

In this Paper, We study the vulnerabilities of a Smart Plug system by reverse engineering its communication protocols. After we obtain the details of its communication protocols, we are able to identify several security vulnerabilities, including insecure communication protocols, lack of device authentication, and a weak password policy. We propose four attacks, device scanning attack, brute force attack, device spoofing attack, and firmware attack, to demonstrate the severity of these security risks. The device scanning attack can find all online plugs. The brute force attack and device spoofing attack can obtain the device password whatever it is. The firmware attack can obtain the root access on the plug system. To thwart these serious threats, we present the guidelines for corresponding countermeasures.

FUTURE-SCOPE

Through these countermeasures, we are able to send a compelling message to all manufacturers of IoT devices to strengthen their security and provide a safe and secure environment for service users. Some of the Security firms are advising consumers to be aware of policy issues related to Smart Plugs and other inter-connected devices. Consumers should do proper research before buying and look at online reviews to see if other users have reported any problems.

ACKNOWLEDGMENT

Primarily I would like to Thank GOD for being able to complete this Paper with success. Then I would like to thank my Parents and Friends who have helped me with their valuable suggestions and guidance which were helpful in various phases of Completion of this Paper. Then, I would like to thank my Guide Prof. S V.Athawale whose valuable guidance has helped me patch this paper and make it a full proof success.

REFERENCES

[1] **Zhen Ling; Junzhou Luo; Yiling Xu; Chao Gao;KuiWu and Xinwen Fu** , "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System", IEEE Internet of Things Journal,2017.
[2] **O. Arias, J. Wurm, K. Hoang, and Y. Jin**, "Privacy and security in internet of things and wearable devices", IEEE Transactions on Multi-Scale Computing Systems, 2015.
[3] **I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, and M. Gruteser**, "Neighborhood watch: Security and privacy analysis of automatic meter reading systems", in Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS), 2016.
[4] **Q. Yang, J. Yang, D. A. W. Yu, N. Zhang, and W. Zhao**, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications", IEEE Internet of Things Journal, 2017.
[5] **S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini**, "Security, privacy and trust in internet of things: The road ahead", Chichester, UK: Wiley-IEEE Press, Computer Networks, 2015.
[6] **M. Rahman, B. Carbunar, and M. Banik**, "Fit and vulnerable: Attacks and defenses for a health monitoring device", in Proceedings of the 34th IEEE Symposium on Security and Privacy (SP), 2014.
[7] **P. Koeberl, S. Schulz, A.-R. Sadeghi, and V. Varadharajan**, "Trustlite: A security architecture for tiny embedded devices", in Proceedings of European Conference on Computer Systems (EuroSys), 2016.